Data protection policy

Aim - Rydal Day Nursery is dedicated to ensuring that all information stored about parents and carers, children and staff are kept as secure as possible at all times and stored in accordance to the Data Protection Act 1998.

Responsibility - This is the overall responsibility of the nursery director to ensure all information is safe and secure and in compliance with the Data Protection Act 1998 however, all staff have a responsibility to ensure information is not shared with any individual outside of the setting.

Principles - In accordance with the data protection Act 1998 Rydal Day Nursery is responsible for following the data protection principles. These make sure information is:

* Used fairly and lawfully

* Used for limited, specifically stated purposes

* Used in a way that is adequate, relevant and not excessive

* Accurate

* Kept for no longer than is absolutely necessary

* Handled according to people's data protection rights

* Kept safe and secure

* Not transferred outside the European area without adequate protection

This also includes more sensitive information such as ethnic background, political opinions, religious beliefs, health, sexual health and criminal records.

Information stored – Person information will be stored in one of two ways, paper form or on the computer in a password secured file. All paper copies of personal information are stored in a locked cupboard in the office with limit access to only staff in the management team and parents on request. Permission to store information on the computer will be sought from parents or staff during registration through the contracts. All computers are password protected and information is also stored in password protected files within the computers. Computers in the office are again only accessed by the management team or if used by another member of the team personal

files are not accessible to them. In line with the updated data protection policy staff have 28 days to provide information on request from a parent or carer.

Personal information that is stored will include:

* Children's and parent's details such as name, address, date of birth, phone numbers, medical information and bank details.

* Staff details such as name, address, medical information, bank details, criminal records, insurance numbers and qualifications.

* Accident forms, incident records, restraint records, administration of medication records.

* Child protection records.

Information Commissioners Office – The Data Protection Act 1998 requires every organisation that processes personal information to register with the Information Commissioner's Office (ICO), unless they are exempt. Failure to do so is a criminal offence. The role of the ICO is to uphold information rights in the public interest and to improve the information rights practices of organisations by gathering and dealing with concerns raised by members of the public. The ICO has set out a commitment to increase consumer trust people have in what happens to their personal data. The Commissioner has also demonstrated a focus on the essential role data protection can play in innovation, and the importance of organisations understanding the growing impetus on companies to be accountable for what they do with personal data. This forms a central part of the new General Data Protection Regulation, which comes into force in May 2018.

Data Protection Officer – A data protection officer (DPO) is a security leadership role required by the General Data Protection Regulation (GDPR). Data Protection Officers are responsible for overseeing data protection strategies and implementations to ensure compliance with GDPR requirements. When the GDPR becomes effective in May 2018 the data protection officer becomes a mandatory role under Article 37 for all companies that collect or process personal data in the EU. DPO's responsibilities include but are not limited to educating the company and its employees on the important compliance requirements and conducting regular security audits. The are also responsible for serving point of contact between the company and GDPR supervisory Authorities. The DPO will need to ensure they have informed parents, carers and staff on how their data is being stored and their rights to any of it being erased at any point.

All parents should note that in an event of a child protection concern then information about children and their families maybe shared with relevant agencies without consent of the parent as supported in the information sharing policy.